Carnegie Mellon University
Software Engineering Institute

The AI Division

Building AI Better

LEADERS IN DEFENSE AND NATIONAL SECURITY ORGANIZATIONS WANT TO OBTAIN THE LEAP-AHEAD CAPABILITIES ARTIFICIAL INTELLIGENCE (AI) OFFERS. At the same time, it is difficult to get AI right. As many as 85% of current AI deployments fail—failures largely due to the difficulty of replicating, verifying, and validating rapidly developed and deployed AI systems.

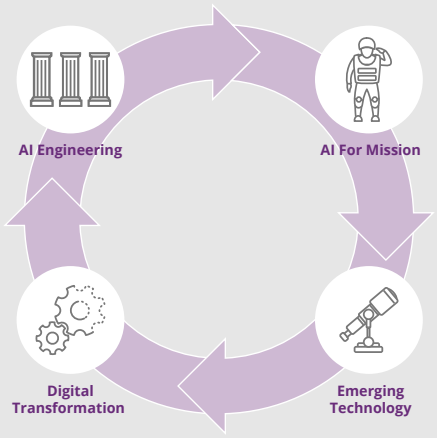
About the AI Division

The SEI AI Division addresses the need for leap-ahead AI capabilities that are reliable, responsible, safe, fair, and transparent. As part of Carnegie Mellon University, a world leader in AI, we are building on our continuing legacy as world experts in cultivating a discipline of software engineering and pioneers in cybersecurity to help our mission partners acquire, build, and deliver AI systems that address mission needs.

What We Do

The SEI AI Division conducts research in applied artificial intelligence with a primary focus on AI Engineering, addressing questions related to the practical design and implementation of AI. As our government mission partners adopt AI and machine learning, we are helping surface leading practices through a community-wide movement to mature the discipline of AI Engineering, leveraging defense and national security problems as a context for definition. In our work, we build real-world, mission-scale AI capabilities, and research and define the processes, practices, and tools to support operationalizing robust, secure, scalable, and human-centered AI systems.

OUR CAPABILITIES



AI ENGINEERING
Research and define the processes, practices, and tools to support operationalizing robust, secure, scalable, and human-centered AI systems.

EMERGING TECHNOLOGY
Identify and investigate emerging AI and AI-adjacent technologies that are rapidly transforming the technology landscape.

AI FOR MISSION
Build real-world, mission-scale AI capabilities.

DIGITAL TRANSFORMATION
Prepare our mission partners to be ready for the unique challenges of adopting, deploying, using, and maintaining AI capabilities.

Our Virtual Labs

We accelerate collaboration through virtual laboratories that enable us to work closely with researchers, stakeholders, and mission partners.

Advanced Computing Lab

Hardware is a key enabler for AI, and the hardware landscape is evolving rapidly. Our advanced computing lab identifies, evaluates, and applies the latest in AI computing technologies to solve DoD and national security problems. We collaborate with mission partners, stakeholders, government organizations, and the defense industrial base to improve existing capabilities and identify future capabilities. Our work spans the entire stack: from algorithms to assembler, across the full computing spectrum, from big iron to the edge.

Adversarial Machine Learning Lab

Our Adversarial Machine Learning Lab is working to make machine learning as secure as possible for the DoD and intelligence community (IC). We organize our work into a find-fix-verify paradigm, where we find machine learning vulnerabilities by developing new adversarial attacks, fix vulnerabilities by developing defenses and mitigations to known attacks, and verify, within a given system, that vulnerabilities have been properly mitigated via adversarially focused test and evaluation. Our portfolio of work ranges from open collaborations with our colleagues at Carnegie Mellon University to restricted collaborations with DoD and IC sponsors.

Featured Research Areas

AI Engineering, A National Initiative: We lead a community-wide initiative to evolve an AI engineering discipline focusing on safety, security, robustness, reliability, resiliency, and ethics.
bit.ly/SEI-AI-Eng

Responsible AI: We co-authored the Defense Innovation Unit's Responsible AI Guidelines, which enable practitioners to put ethical AI principles into practice.
bit.ly/DIU-Responsible-AI

Adversarial Machine Learning: We are developing new methods to identify, prioritize, and prevent adversarial attacks on ML algorithms.
bit.ly/SEI-TBV

Edge AI: We are meeting challenges in the fields of performance engineering, embedded systems, and machine learning to move AI onto small devices with limited power.
bit.ly/SEI-Edge-AI

AI Uncertainty: We are developing new techniques to accurately estimate uncertainty in ML models, detect domain shift, provide efficient retraining mechanisms, and reason in the open world.
bit.ly/SEI-AI-Uncertainty

About the SEI

The Software Engineering Institute is a federally funded research and development center (FFRDC) that works with defense and government organizations, industry, and academia to advance the state of the art in software engineering and cybersecurity to benefit the public interest. Part of Carnegie Mellon University, the SEI is a national resource in pioneering emerging technologies, cybersecurity, software acquisition, and software lifecycle assurance.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu

©2022 Carnegie Mellon University | 5861 | 04.15.2022 | DM22-0357